

An Upper Bound on the Sizes of Multiset-Union-Free Families

Or Ordentlich and Ofer Shayevitz *

Abstract

Let \mathcal{F}_1 and \mathcal{F}_2 be two families of subsets of an n -element set. We say that \mathcal{F}_1 and \mathcal{F}_2 are multiset-union-free if for any $A, B \in \mathcal{F}_1$ and $C, D \in \mathcal{F}_2$ the multisets $A \uplus C$ and $B \uplus D$ are different, unless both $A = B$ and $C = D$. We derive a new upper bound on the maximal sizes of multiset-union-free pairs, improving a result of Urbanke and Li.

1 Introduction

Let \mathcal{F}_1 and \mathcal{F}_2 be two families of subsets of an n -element set. We say that \mathcal{F}_1 and \mathcal{F}_2 are *multiset-union-free* if the multiset union of the families \mathcal{F}_1 and \mathcal{F}_2 , defined as

$$\mathcal{F}_1 \uplus \mathcal{F}_2 \triangleq \{F_1 \uplus F_2 : F_1 \in \mathcal{F}_1, F_2 \in \mathcal{F}_2\} \quad \text{with multiplicities}$$

contains exactly $|\mathcal{F}_1| \cdot |\mathcal{F}_2|$ distinct elements. It would sometimes be instructive to represent \mathcal{F}_i by the corresponding set \mathcal{C}_i of binary characteristic vectors; the multiset-union-free property is then equivalent to the requirement that $\mathbf{a} + \mathbf{c} \neq \mathbf{b} + \mathbf{d}$ for any vectors $\mathbf{a}, \mathbf{b} \in \mathcal{C}_1$ and $\mathbf{c}, \mathbf{d} \in \mathcal{C}_2$ unless both $\mathbf{a} = \mathbf{b}$ and $\mathbf{c} = \mathbf{d}$, where addition is over the reals. We say that a pair $0 \leq R_1 \leq 1$, $0 \leq R_2 \leq 1$ is admissible if there exists a sequence of multiset-union-free pairs \mathcal{F}_1 and \mathcal{F}_2 with cardinalities $|\mathcal{F}_1| = 2^{n(R_1+o(1))}$ and $|\mathcal{F}_2| = 2^{n(R_2+o(1))}$. Our goal is to find necessary conditions for a pair (R_1, R_2) to be admissible. The set of all admissible (R_1, R_2) has been extensively studied in the information theory literature; it is often referred to as the zero-error capacity region of the binary adder channel [1–10].

*The authors are with the Department of Electrical Engineering - Systems at the Tel Aviv University, {ordent,ofersha}@eng.tau.ac.il. The work of O. Ordentlich was supported by the Admas Fellowship Program of the Israel Academy of Science and Humanities, a fellowship from The Yitzhak and Chaya Weinstein Research Institute for Signal Processing at Tel Aviv University, and the Feder Family Award. The work of O. Shayevitz was supported in part by the Marie Curie Career Integration Grant (CIG), Grant agreement no. 631983, and in part by the Israel Science Foundation under Grant No. 1367/14.

Clearly, $R_1 + R_2 \leq \log 3 \approx 1.5849$ must hold, where logarithms are taken in base 2. This bound can be easily improved via standard information theoretic arguments. Recall that the entropy of a random variable X with a probability distribution $P = (p_1, \dots, p_K)$ is

$$H(X) = - \sum_k p_k \log p_k.$$

When convenient, we also denote the entropy of X above by $H(P)$. Assume $\mathcal{F}_1, \mathcal{F}_2$ are multiset-union-free families with cardinalities 2^{nR_1} and 2^{nR_2} respectively. Let $\mathbf{X}_1, \mathbf{X}_2$ be two characteristic vectors pertaining to subsets in $\mathcal{F}_1, \mathcal{F}_2$ respectively chosen uniformly at random, independently of each other. The real sum $\mathbf{X}_1 + \mathbf{X}_2$ is hence uniformly distributed over all $|\mathcal{F}_1| \cdot |\mathcal{F}_2| = 2^{n(R_1+R_2)}$ possible sums. By the subadditivity of entropy [11]

$$n(R_1 + R_2) = H(\mathbf{X}_1 + \mathbf{X}_2) \leq \sum_{k=1}^n H(X_{1,k} + X_{2,k}) \leq n \cdot \max_{P_{X_1}, P_{X_2}} H(X_1 + X_2)$$

where the maximization is over all independent binary random variables X_1, X_2 . The maximum is attained for uniform P_{X_1} and P_{X_2} , which yields the bound $R_1 + R_2 \leq \frac{3}{2}$.

Write $h(p) = H(p, 1-p)$ for the binary entropy, and $h^{-1}(x)$ for its inverse restricted to $[0, \frac{1}{2}]$. To date, the only improvement over the simple bound above was given by Urbanke and Li:

Theorem 1 (Urbanke and Li [8]). *Any admissible (R_1, R_2) satisfies*

$$R_1 + R_2 \leq \min_{0 \leq \rho \leq \frac{1}{2}} \max_{0 \leq \kappa \leq 1} h(\langle 1 - h^{-1}(R_1) - \kappa \rangle) - h(\rho) + \min \{g^*(\rho), \langle \rho + \kappa \rangle + h(\langle \rho + \kappa \rangle)\}$$

where $\langle a \rangle \triangleq \min(a, 1/2)$, and

$$g^*(\rho) = \max_{0 \leq \beta \leq 1} h(((1-\rho)(1-\beta), \rho(1-\beta) + (1-\rho)\beta, \rho\beta)).$$

For the maximal value of $R_1 = 1$, this bound yields $R_2 < 0.49216$, which improves upon $R_2 \leq 0.5$ given by the standard information theoretic bound.

For $0 \leq p, q \leq 1$, write $p \star q \triangleq p(1-q) + q(1-p)$. Let

$$\begin{aligned} L(\eta) &\triangleq h(\eta) + 1 - \eta \\ J(p, \eta) &\triangleq \begin{cases} 2h\left(\frac{1}{2}(1 - \sqrt{1-2\eta})\right) - \eta & \eta \geq p \star p \\ 2h\left(\frac{1}{2}\left(1 - \frac{1-\eta-p\star p}{\sqrt{1-2(p\star p)}}\right)\right) - \frac{1}{2}\left(1 - \frac{(1-\eta-p\star p)^2}{1-2(p\star p)}\right) & \eta < p \star p \end{cases} \end{aligned} \quad (1)$$

and

$$R_\Sigma(r_0, r_1) \triangleq \max_{h^{-1}(r_1) \leq \eta \leq \frac{1}{2}} \min\{L(\eta), J(h^{-1}(r_1), \eta) + r_0\} \quad (2)$$

Our main result is the following.

Theorem 2. Any admissible (R_1, R_2) satisfies

$$R_2 < \min_{0 \leq \alpha \leq h^{-1}(R_1)} (1 - \alpha) \left(R_\Sigma \left(\frac{\alpha}{1 - \alpha}, \Gamma(R_1, \alpha) \right) - \Gamma(R_1, \alpha) \right)$$

where

$$\Gamma(R_1, \alpha) \triangleq h \left(\frac{h^{-1}(R_1) - \alpha}{1 - \alpha} \right)$$

For the maximal value of $R_1 = 1$, this bound yields $R_2 < 0.4798$, which improves upon Theorem 1. Figure 1 depicts the three bounds for values of R_1 close to 1.

The question of whether $R_1 + R_2 = \frac{3}{2}$ is admissible for some (R_1, R_2) remains wide open. We also note that there is a large gap between our bound and the best known constructions. For $R_1 = 1$, only $R_2 = \frac{1}{4}$ is known to be admissible [5], and the best known construction for the sum [10] yields $R_1 + R_2 \approx 1.31781$.

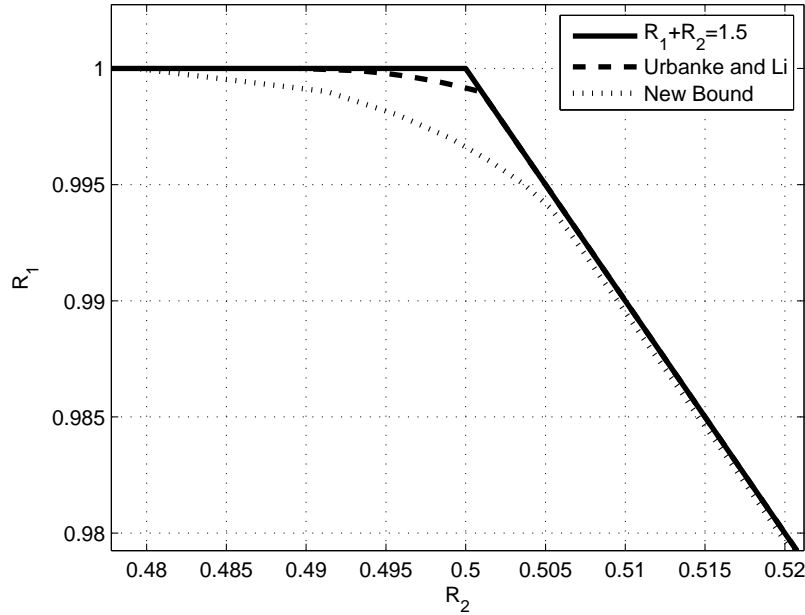


Figure 1: Illustration of the three bounds.

2 Proof of Theorem 2

To avoid cumbersome notations, and since admissibility is an asymptotic property, we can assume without loss of generality that nR_1 and nR_2 (and all similar quantities) are integers.

2.1 Motivation

Let \mathcal{F} be a family of subsets of $[n] \triangleq \{1, \dots, n\}$, and $S \subseteq [n]$. We say that S is *shattered* by \mathcal{F} [12], if the *projection multiset* (or simply *projection*)

$$P_S^+(\mathcal{F}) \triangleq \{F \cap S : F \in \mathcal{F}\} \quad \text{with multiplicities}$$

of \mathcal{F} on S contains all subsets of S .¹ A family \mathcal{F} is said to be *systematic* if it is shattered by some $S \subseteq [n]$ of cardinality $\log |\mathcal{F}|$. Weldon proved the following [4].

Theorem 3 (Weldon [4]). *If \mathcal{F}_1 is systematic and the pair $\mathcal{F}_1, \mathcal{F}_2$ is multiset-union-free, then $R_2 \leq (1 - R_1) \log 3$.*

Proof. Let S be a set of cardinality nR_1 that is shattered by \mathcal{F}_1 . For every $F_2 \in \mathcal{F}_2$, there exists an $F_1 \in \mathcal{F}_1$ such that F_1 and F_2 are an S -complement pair, i.e.,

$$(F_1 \cap S) \uplus (F_2 \cap S) = S. \quad (3)$$

Hence, there are at least 2^{nR_2} such S -complement pairs. By the multiset-union-free assumption, $(F_1 \cap S) \uplus (F_2 \cap S)$ must be distinct for all S -complement pairs. Therefore, the number of such pairs cannot be larger than $3^{|S|} = 3^{n(1-R_1)}$, and the theorem follows. \square

For example, if \mathcal{F}_1 is systematic and $R_2 = 1$, then the theorem implies that $R_1 \leq 0.37$. This strong bound is a consequence of the restriction to a systematic family. However, we note that the only property used in the proof is the existence of a large shattered set. Hence, any lower bound on the size of a maximal shattered set in a general family \mathcal{F}_1 would lead to a similar result. The Sauer-Perles-Shelah lemma provides such a guarantee.

Lemma 1 (Sauer-Perles-Shelah [12]). *Let \mathcal{F} be a family of subsets on an n -element set. If the cardinality of the maximal subset shattered by \mathcal{F} is d , then $|\mathcal{F}| \leq \sum_{k=0}^d \binom{n}{k}$.*

Remark 1. *It is easy to see that this bound is attained with equality if \mathcal{F} is a n -Hamming ball of radius d .*

Corollary 1. *Let $\varepsilon > 0$. If $|\mathcal{F}| = 2^{n(R+\varepsilon)}$ then for any n large enough, \mathcal{F} shatters a set $S \subseteq [n]$ with $|S| \geq nh^{-1}(R)$.*

Plugging the above into Weldon's argument yields:

Proposition 1. *If the pair $\mathcal{F}_1, \mathcal{F}_2$ is multiset-union-free, then $R_2 \leq (1 - h^{-1}(R_1)) \log 3$.*

Unfortunately, this bound is trivial since $R_1 + (1 - h^{-1}(R_1)) \log 3 > \frac{3}{2}$ for any R_1 . This stems from two main weaknesses. First, we have taken the worse case assumption that each subset $F_2 \in \mathcal{F}_2$ has only one subset $F_1 \in \mathcal{F}_1$ such that F_1 and F_2 are S -complement, where S is a shattered set in \mathcal{F}_1 . Second, bounding the number of S -complement pairs by $3^{|S|}$ may be loose, as it ignores the multiset union structure. In the next two subsections, we provide the technical tools to handle each of these weaknesses. We then apply them to prove the theorem in the subsection that follows.

¹Taking the multiplicities into account in the definition of the projection is not necessary here, but will become important in the sequel.

2.2 A Soft Sauer-Perles-Shelah Lemma

Let \mathcal{F} be a family of subsets of $[n] \triangleq \{1, \dots, n\}$, and $S \subseteq [n]$. We say that S is k -shattered by \mathcal{F} , if the projection multiset $P_S^+(\mathcal{F})$ of \mathcal{F} on S contains all subsets of S each with multiplicity of at least k . For $k = 1$, this definition reduces to the regular definition of a shattered set.

In Section 3, we prove the following Lemma.

Lemma 2. *Let \mathcal{F} be a family of subsets of an n -element set. If the cardinality of the maximal subset that is k -shattered by \mathcal{F} is $d - 1$, then*

$$|\mathcal{F}| \leq \sum_{t=1}^{t^*} \binom{n}{t} + \binom{n}{t^*} \sum_{t=t^*+1}^n \frac{\binom{t^*}{d}}{\binom{t}{d}}$$

where t^* is the smallest integer t satisfying $\binom{n-d}{t-d} \geq k$ if such an integer exists, and $t^* = n$ otherwise.

Remark 2. Note that if $k = \binom{n-d}{t^*-d}$ for some t^* , then our bound is tight for a n -Hamming ball of radius t^* , up to multiplicative gap of $O(n/d)$. This coincides with the Sauer-Perles-Shelah Lemma for $k = 1$ (and $t^* = d$), up to the aforementioned multiplicative factor. Since we are only interested in exponential behavior, no attempt has been made to reduce this gap.

Corollary 2. *Let $\varepsilon > 0$. If $|\mathcal{F}| = 2^{n(R+\varepsilon)}$ then for any $0 \leq \alpha \leq h^{-1}(R)$ and any n large enough, there exists a set $S \subseteq [n]$ with $|S| \geq n\alpha$ that is $2^{n\beta}$ -shattered by \mathcal{F} , where*

$$\beta = (1 - \alpha) \cdot h \left(\frac{h^{-1}(R) - \alpha}{1 - \alpha} \right) \quad (4)$$

Proof. Let $0 \leq \alpha \leq h^{-1}(R)$ and assume to the contrary that the claim does not hold. Denote $t^* = \gamma_n n$, and write

$$\begin{aligned} \frac{1}{n} \log \binom{n-d}{t^*-d} &= \frac{n-d}{n} \left(h \left(\frac{t^*-d}{n-d} \right) + o(1) \right) \\ &= (1 - \alpha + o(1)) h \left(\frac{\gamma_n - \alpha + o(1)}{1 - \alpha + o(1)} \right) \end{aligned}$$

We can set γ_n to the minimal value guaranteeing that the above is at least β , which is $\gamma_n = \alpha + (1 - \alpha)h^{-1} \left(\frac{\beta}{1 - \alpha} \right) + o(1)$. Invoking Lemma 2, it must then be that $|\mathcal{F}| > 2^{n(h(\gamma_n) + o(1))} = 2^{n(R + o(1))}$, contradicting the assumption. \square

2.3 An Information Theoretic Lemma

We define a natural generalization of the multiset-union-free property for sets of family pairs. A *system* \mathcal{U} is a set of pairs $\{\mathcal{F}_{1,i}, \mathcal{F}_{2,i}\}_{i=1}^{M_0}$, where each $\mathcal{F}_{1,i}$ (resp. $\mathcal{F}_{2,i}$) is a family

of subsets of $[n]$ with fixed cardinality $|\mathcal{F}_{1,i}| = M_1$ (resp. $|\mathcal{F}_{2,i}| = M_2$). We say that \mathcal{U} is a *multiset-union-free system* if each pair $(\mathcal{F}_{1,i}, \mathcal{F}_{2,i})$ is multiset-union-free, and the families of multisets $\mathcal{F}_{1,i} \uplus \mathcal{F}_{2,i}$ are mutually disjoint.

A triplet (r_0, r_1, r_2) is called admissible if there exists a sequence of multiset-union-free systems \mathcal{U} with $M_\ell = 2^{n(r_\ell + o(1))}$ for $\ell \in \{0, 1, 2\}$. The goal of this subsection is to provide a necessary condition for a triplet to be admissible. In the Weldon-type arguments mentioned above, the number of S -complement pairs was bounded by $3^{|\bar{S}|}$, thereby ignoring the multiset union structure. As we shall see in the next subsection, this structure can be accounted for by partitioning each family according to its projection on S , which naturally gives rise to a system with $r_0 \leq |S|/|\bar{S}|$. Moreover, any upper bound on the corresponding admissible sum $r_0 + r_1 + r_2$ can be translated into an upper bound on the number of S -complement pairs in our original setup.

For $r_0 = 0$, the problem coincides with the standard multiset-union-free problem, for which $r_0 + r_1 + r_2 \leq \frac{3}{2}$ follows from the information theoretic argument given in Section 1. It is also easy to see that for a large enough value of r_0 , the sum $r_0 + r_1 + r_2 = \log 3$ is admissible. For example, let $\mathcal{F}_0 = \{F_{0,1}, \dots, F_{0,M_0}\}$ be the set of all subsets of $[n]$ with cardinality $2n/3$, and identify each pair $\{\mathcal{F}_{1,i}, \mathcal{F}_{2,i}\}$ in the system \mathcal{U} with one of these subsets. Let $\mathcal{F}_{1,i} = \{F_{0,i}\}$ and $\mathcal{F}_{2,i} = \{F \subset [n] : F \subseteq F_{0,i}\}$. Clearly, each pair $(\mathcal{F}_{1,i}, \mathcal{F}_{2,i})$ is multiset-union-free, and moreover, the families of multisets $\mathcal{F}_{1,i} \uplus \mathcal{F}_{2,i}$ as defined above are disjoint, as exactly all the elements of $F_{0,i}$ participate in each corresponding family of multisets. For this construction, $r_0 = \frac{1}{n} \log \binom{n}{2n/3} \approx h(\frac{1}{3})$, $r_1 = 0$ and $r_2 = \frac{2}{3}$, hence in the limit of large n this construction yields $r_0 + r_1 + r_2 = \log 3$. The next lemma refines these observations by upper bounding admissible sums $r_0 + r_1 + r_2$ between $\frac{3}{2}$ and $\log 3$, as a function of r_0 and r_1 . The proof appears in Section 4.

Lemma 3. *Let $L(\eta)$ and $J(p, \eta)$ be as defined in (1). If (r_0, r_1, r_2) is admissible, then*

$$r_0 + r_1 + r_2 \leq \max_{h^{-1}(r_1) \leq \eta \leq \frac{1}{2}} \min\{L(\eta), J(h^{-1}(r_1), \eta) + r_0\}$$

Remark 3. *Note that it can be shown that the maximization can be further restricted to $h^{-1}(r_1) \star h^{-1}(r_2) \leq \eta \leq \frac{1}{2}$. This however is not useful for our purposes.*

2.4 Putting it Together

We are now in a position to prove Theorem 2. Let $\mathcal{F}_1, \mathcal{F}_2$ be a pair of multiset-union-free families of cardinalities 2^{nR_1} and 2^{nR_2} respectively. Given this pair, we use Corollary 2 to construct a multiset-union-free system with certain cardinalities, and then apply Lemma 3 to obtain constraints on that system.

By Corollary 2, for any $\alpha < h^{-1}(R_1)$ there exists a subset $S \subset [n]$ of cardinality $n\alpha$ that is $2^{n\beta}$ -shattered by \mathcal{F}_1 , where β is given in (4), all up to an $o(1)$ term. Let \mathcal{F}_0 be the family of all subsets of S , and for any $G \in \mathcal{F}_0$ let $\mathcal{F}_{1,G} = \{F \in \mathcal{F}_1 : F \cap S = G\}$. Define $\mathcal{F}_{2,G}$ similarly, and note that $\{\mathcal{F}_{i,G}\}_{G \in \mathcal{F}_0}$ is a partition of \mathcal{F}_i for each $i \in \{1, 2\}$.

By construction, $|\mathcal{F}_{1,G}| \geq 2^{n\beta}$. We can therefore arbitrarily choose $\tilde{\mathcal{F}}_{1,G} \subseteq \mathcal{F}_{1,G}$ such that $|\tilde{\mathcal{F}}_{1,G}| = 2^{n\beta}$. For each G with $|\mathcal{F}_{2,G}| > 0$, arbitrarily choose $\tilde{\mathcal{F}}_{2,G} \subseteq \mathcal{F}_{2,G}$ such that $\log |\tilde{\mathcal{F}}_{2,G}| = \lfloor \log |\mathcal{F}_{2,G}| \rfloor$. Note that this guarantees that $|\tilde{\mathcal{F}}_{2,G}| = 2^k$ for some integer $0 \leq k \leq nR_2$, and that $|\tilde{\mathcal{F}}_{2,G}| \geq |\mathcal{F}_{2,G}|/2$. Moreover, there must exist an integer k' with the property that the union of all $\tilde{\mathcal{F}}_{2,G}$ of cardinality $2^{k'}$ contains at least $\frac{1}{2(nR_2+1)}2^{nR_2}$ subsets. Let \mathcal{G} be the set of all $G \in \mathcal{F}_0$ that correspond to this k' , and note that by construction $|\mathcal{G}| = 2^{n\alpha'}$ for some $\alpha' \leq \alpha$. Moreover, $|\tilde{\mathcal{F}}_{2,G}| = 2^{k'} \geq \frac{1}{2(nR_2+1)}2^{n(R_2-\alpha')}$ for all $G \in \mathcal{G}$.

Let $\bar{G} = S \setminus G$, and define the system $\mathcal{U} = \{(\tilde{\mathcal{F}}_{1,\bar{G}}, \tilde{\mathcal{F}}_{2,G})\}_{G \in \mathcal{G}}$. Since the original \mathcal{F}_1 and \mathcal{F}_2 are multiset-union-free, then \mathcal{U} is trivially a multiset-union-free system. Moreover, since any $F_1 \in \tilde{\mathcal{F}}_{1,\bar{G}}$ and $F_2 \in \tilde{\mathcal{F}}_{2,G}$ are an S -complement pair (3), the projection² $\mathcal{U}_{\bar{S}} = \{(P_{\bar{S}}^+(\tilde{\mathcal{F}}_{1,\bar{G}}), P_{\bar{S}}^+(\tilde{\mathcal{F}}_{2,G}))\}_{G \in \mathcal{G}}$ of \mathcal{U} onto \bar{S} is also a multiset-union-free system, over $|\bar{S}| = n(1-\alpha)$ elements.

We have thus shown that given a multiset-union-free pair over $[n]$ with cardinalities 2^{nR_1} and 2^{nR_2} , we can construct a multiset-union-free system $\mathcal{U}_{\bar{S}}$ over $[m] = [n(1-\alpha)]$ with cardinalities $M_0 = 2^{mr_0}$, $M_1 = 2^{mr_1}$ and $M_2 = 2^{m(r_2+o(1))}$, where $r_0 = \frac{\alpha'}{1-\alpha}$, $r_1 = \frac{\beta}{1-\alpha}$ and $r_2 = \frac{R_2-\alpha'}{1-\alpha}$. Thus for this system $r_0 + r_1 + r_2 = \frac{R_2+\beta}{1-\alpha}$, and by Lemma 3 we have that

$$\frac{R_2 + \beta}{1 - \alpha} \leq \max_{h^{-1}(\frac{\beta}{1-\alpha}) \leq \eta \leq \frac{1}{2}} \min \left\{ L(\eta), J \left(h^{-1} \left(\frac{\beta}{1-\alpha} \right), \eta \right) + \frac{\alpha'}{1-\alpha} \right\},$$

where we have used $\alpha \leq \alpha$. The theorem now follows by substituting β from Corollary 2, and noting that the inequality above holds for any $0 \leq \alpha \leq h^{-1}(R_1)$.

3 Proof of Lemma 2

Let \mathcal{F} be a family of subsets on $[n]$. We start by applying the shifting argument introduced in [13], to construct another family \mathcal{G} of the same cardinality, such that if S is k -shattered by \mathcal{G} then it is also k -shattered by \mathcal{F} . Furthermore, \mathcal{G} will be *monotone*, i.e., will have the property that if $G \in \mathcal{G}$ then all subsets of G are in \mathcal{G} .

Set $\mathcal{G} = \mathcal{F}$. If \mathcal{G} is already monotone, we are done. Otherwise there exists some $i \in [n]$ such that the set $\tilde{\mathcal{G}}_i = \{G \in \mathcal{G} : i \in G, G \setminus \{i\} \notin \mathcal{G}\}$ is not empty. Update \mathcal{G} according to the rule:

$$\mathcal{G} \leftarrow (\mathcal{G} \setminus \tilde{\mathcal{G}}_i) \cup (\tilde{\mathcal{G}}_i - i) \quad (5)$$

where $\tilde{\mathcal{G}}_i - i$ is the family of subsets obtained from $\tilde{\mathcal{G}}_i$ by removing the element i from each subset. The process continues until \mathcal{G} is monotone, and is clearly guaranteed to terminate in finite time. By construction, $|\mathcal{G}| = |\mathcal{F}|$.

²Note that $P_{\bar{S}}^+(\tilde{\mathcal{F}}_{1,\bar{G}})$ and $P_{\bar{S}}^+(\tilde{\mathcal{F}}_{2,G})$ have no multiplicities.

We now show that if S is k -shattered by \mathcal{G} then it is also k -shattered by \mathcal{F} . Let \mathcal{G}' be the family of subsets before the operation (5) on some element i , and let \mathcal{G} be the family obtained after that operation. Suppose S is k -shattered by \mathcal{G} . It now suffices to show that S is also k -shattered by \mathcal{G}' . If $i \notin S$ then clearly $P_S^+(\mathcal{G}) = P_S^+(\mathcal{G}')$, hence this does not affect the k -shatteredness of S . Suppose $i \in S$, and let $\mathcal{G}_i = \{G \in \mathcal{G} : i \in G\}$. Then $\mathcal{G}_i \subseteq \mathcal{G}'$ since the update rule (5) does not add elements to subsets. Since \mathcal{G} k -shatters S , then every subset of S that contains i has multiplicity at least k in $P_S^+(\mathcal{G}_i) \subseteq P_S^+(\mathcal{G}')$. Recalling that $\mathcal{G}_i \subseteq \mathcal{G} \cap \mathcal{G}'$, we have that $\mathcal{G}_i - i \subseteq \mathcal{G}'$ since otherwise some replacement would have occurred in (5). Since \mathcal{G} k -shatters S , then every subset of S that does not contain i has multiplicity at least k in $P_S^+(\mathcal{G}_i - i) \subseteq P_S^+(\mathcal{G}')$.

The Lemma now follows directly from the next proposition.

Proposition 2. *If \mathcal{G} is a monotone family of subsets of $[n]$ with the property that no subset of cardinality d is k -shattered by \mathcal{G} , then*

$$|\mathcal{G}| \leq \sum_{t=1}^{t^*} \binom{n}{t} + \binom{n}{t^*} \sum_{t=t^*+1}^n \frac{\binom{t^*}{d}}{\binom{t}{d}}$$

where t^* is the smallest integer t satisfying $\binom{n-d}{t-d} \geq k$ if such an integer exists, and $t^* = n$ otherwise.

Proof. Let \mathcal{G}_t denote the family of all subsets in \mathcal{G} with cardinality t . For $t \geq d$, every $G \in \mathcal{G}_t$ has exactly $\binom{t}{d}$ subsets of cardinality d . There is a total of $\binom{n}{d}$ subsets of cardinality d . Hence by a simple counting argument there must exist at least one subset S of cardinality d , that is a subset of no less than $|\mathcal{G}_t| \binom{t}{d} / \binom{n}{d}$ subsets in \mathcal{G}_t . Recalling that \mathcal{G} is monotone, this implies that S is $|\mathcal{G}_t| \binom{t}{d} / \binom{n}{d}$ -shattered by \mathcal{G} . By our assumption, it must be that

$$\frac{\binom{t}{d} |\mathcal{G}_t|}{\binom{n}{d}} < k, \quad t = d, \dots, n$$

On the other hand, $|\mathcal{G}_t| \leq \binom{n}{t}$, and therefore

$$|\mathcal{G}_t| \leq \min \left\{ \binom{n}{t}, \frac{\binom{n}{d} k}{\binom{t}{d}} \right\}, \quad t = d, \dots, n$$

Summing over t we get

$$|\mathcal{G}| = \sum_{t=1}^n |\mathcal{G}_t| \leq \sum_{t=1}^{d-1} \binom{n}{t} + \sum_{t=d}^n \min \left\{ \binom{n}{t}, \frac{\binom{n}{d} k}{\binom{t}{d}} \right\} \quad (6)$$

Let t^* be the smallest integer t such that $\binom{n}{t} \geq \frac{\binom{n}{d} k}{\binom{t}{d}}$ if such an integer exists. If no such integer t exists, set $t^* = n$. Then

$$|\mathcal{G}| \leq \sum_{t=1}^{t^*} \binom{n}{t} + \sum_{t=t^*+1}^n \frac{\binom{n}{d} k}{\binom{t^*}{d}} \cdot \frac{\binom{t^*}{d}}{\binom{t}{d}} \leq \sum_{t=1}^{t^*} \binom{n}{t} + \binom{n}{t^*} \sum_{t=t^*+1}^n \frac{\binom{t^*}{d}}{\binom{t}{d}}$$

To complete the proof, note that for any $d \leq t \leq n$ we have $\binom{n}{t} \binom{t}{d} = \binom{n}{d} \binom{n-d}{t-d}$, hence t^* is the smallest integer t satisfying $\binom{n-d}{t-d} \geq k$ if such an integer exists, and otherwise $t^* = n$. \square

4 Proof of Lemma 3

We will need the following basic definitions and properties of entropy [11]. The entropy of $X \sim \text{Uniform}([m])$ is $H(X) = \log m$. If $P = (p_0, p_1, \dots, p_k)$ then the grouping rule for entropy states that $H(P) = H(p_0, \dots, p_{k-2}, p_{k-1} + p_k) + (p_{k-1} + p_k)h\left(\frac{p_{k-1}}{p_{k-1} + p_k}\right)$. In particular, if $P = (p_0, p_1, p_2)$, this implies that $H(P) \leq h(p_0) + 1 - p_0$ with equality if and only if $p_1 = p_2$. For two jointly distributed random variables X, Y , let $H(X|Y = y)$ denote the entropy of the distribution $P_{X|Y=y}$, and let $H(X|Y)$ be its expectation w.r.t. P_Y . The chain rule for entropies states that $H(X, Y) = H(Y) + H(X|Y)$. In addition, $H(X|Y) \leq H(X)$, i.e., conditioning reduces entropy. The latter two properties imply the sub-additivity of entropy, i.e., $H(X, Y) \leq H(X) + H(Y)$. Finally, note that the binary entropy function $h(\cdot)$ is symmetric around $\frac{1}{2}$.

Let $\mathcal{V} = \{\mathcal{F}_{1,i}, \mathcal{F}_{2,i}\}_{i=1}^{2^{nr_0}}$ be a *multiset-union-free system*, where each $\mathcal{F}_{1,i}$ (resp. $\mathcal{F}_{2,i}$) is a family of subsets of $[n]$ with fixed cardinality $|\mathcal{F}_{1,i}| = 2^{nr_1}$ (resp. $|\mathcal{F}_{2,i}| = 2^{nr_2}$). Let $V \sim \text{Uniform}([2^{nr_0}])$ be an index in the system, chosen uniformly at random. Let $\mathbf{X}_1 \sim \text{Uniform}(\mathcal{C}_{1,V})$ and $\mathbf{X}_2 \sim \text{Uniform}(\mathcal{C}_{2,V})$, where $\mathcal{C}_{j,V}$ is the set of characteristic vectors corresponding to $\mathcal{F}_{j,V}$. Note that this construction induces a joint distribution $P_{V, \mathbf{X}_1, \mathbf{X}_2} = P_V P_{\mathbf{X}_1|V} P_{\mathbf{X}_2|V}$. Let $Q \sim \text{Uniform}([n])$ be a random coordinate of the characteristic vectors, mutually independent of $(\mathbf{X}_1, \mathbf{X}_2, V)$, and define the binary random variables $X_1 = X_{1,Q}$ and $X_2 = X_{2,Q}$.

By the multiset-union-free assumption, we have that $\mathbf{X}_1 + \mathbf{X}_2$ is uniformly distributed over a set of cardinality $2^{n(r_0+r_1+r_2)}$. Using that and the sub-additivity of entropy, we have that

$$\begin{aligned} n(r_0 + r_1 + r_2) &= H(\mathbf{X}_1 + \mathbf{X}_2) \leq \sum_{q=1}^n H(X_{1,q} + X_{2,q}) = n\mathbb{E}H(X_{1,Q} + X_{2,Q}) \\ &= nH(X_1 + X_2|Q) \leq nH(X_1 + X_2) \end{aligned} \quad (7)$$

where the last inequality follows since conditioning reduces entropy. Similarly, we have that $n(r_1 + r_2) = H(\mathbf{X}_1 + \mathbf{X}_2|V = v)$ for any $V = v$, and hence

$$\begin{aligned} n(r_1 + r_2) &= 2^{-nr_0} \sum_{v=1}^{2^{nr_0}} H(\mathbf{X}_1 + \mathbf{X}_2|V = v) = H(\mathbf{X}_1 + \mathbf{X}_2|V) \\ &\leq \sum_{q=1}^n H(X_{1,q} + X_{2,q}|V) = nH(X_2 + X_1|V, Q) \end{aligned} \quad (8)$$

Finally, we also have that $nr_1 = H(\mathbf{X}_1|V = v)$ for any $V = v$ and hence

$$\begin{aligned} nr_1 &= 2^{-nr_0} \sum_{v=1}^{2^{nr_0}} H(\mathbf{X}_1|V = v) = H(\mathbf{X}_1|V) \\ &\leq \sum_{q=1}^n H(X_{1,q}|V) = nH(X_1|V, Q). \end{aligned} \quad (9)$$

Combining (7), (8) and (9), and defining $U = (V, Q)$, we obtain the following.

Proposition 3. *If (r_0, r_1, r_2) is admissible, then there exists $U \sim P_U$ of finite cardinality, and conditional binary distributions $P_{X_1|U}$ and $P_{X_2|U}$, such that*

$$\begin{aligned} r_0 + r_1 + r_2 &\leq H(X_1 + X_2) \\ r_1 + r_2 &\leq H(X_1 + X_2|U) \\ r_1 &\leq H(X_1|U) \end{aligned} \quad (10)$$

where $P_{U, X_1, X_2} = P_U P_{X_1|U} P_{X_2|U}$.

Remark 4. *The above proposition is a special case of a general result of Slepian and Wolf [14].*

Following the proposition above, characterizing the set of all possible entropy triplets $(H(X_1 + X_2), H(X_1 + X_2|U), H(X_1|U))$ will result in necessary conditions for admissibility of triplets (r_0, r_1, r_2) . More precisely, it is our goal to characterize the set of *extremal entropy triplets*, namely those entropy triplets that are Pareto optimal. We refer to the distributions $P_U, P_{X_1|U}, P_{X_2|U}$ that achieve these extremal entropy triplets as *extremal distributions*.

Remark 5. *Using the Carathéodory's Theorem based technique initiated in [15–17], it can be shown that it suffices to consider U of cardinality at most 3. While this significantly reduces the dimension of the space of extremal distributions, the remaining number of parameters still renders a brute-force search prohibitive. Instead, in what follows we bound the extremal entropy triplets analytically.*

First, note that choosing $U = \emptyset$ and X_1, X_2 uniformly random, yields $H(X_1|U) = 1$ and $H(X_1 + X_2|U) = H(X_1 + X_2) = \frac{3}{2}$, with $P_{X_1+X_2}(1) = \frac{1}{2}$. By the grouping property of entropy, if $P_{X_1+X_2}(1) > \frac{1}{2}$ then $H(X_1 + X_2|U) \leq H(X_1 + X_2) < \frac{3}{2}$, hence any extremal distribution must satisfy $P_{X_1+X_2}(1) \leq \frac{1}{2}$. Furthermore, we show the following.

Lemma 4. *Any extremal entropy triplet can be achieved by an extremal distribution inducing a P_{X_1, X_2} that can be described by*

$$X_1 \sim \text{Bern}(\frac{1}{2}), \quad X_2 = X_1 \oplus Z, \quad Z \sim \text{Bern}(\eta) \quad (11)$$

for some $\eta \in [0, \frac{1}{2}]$, where X_1 and Z are independent.

Proof. Consider any choice of P_U , $P_{X_1|U}$ and $P_{X_2|U}$, and without loss of generality assume the support of U is the set $[m]$, for some finite m . We write t_u, q_u for the Bernoulli parameters of $X_1|U = u$ and $X_2|U = u$ respectively. We construct another distribution satisfying (11) that keeps the conditional entropies constant while not decreasing $H(X_1 + X_2)$.

Define an extended distribution W with support $[m] \cup (-[m])$, such that $P_W(w) = \frac{1}{2}P_U(|w|)$. Define further $\tilde{t}_w = t_w$ for $w > 0$ and $\tilde{t}_w = 1 - t_w$ otherwise. Let \tilde{q}_w be defined similarly. With some abuse of notation, let $P_{X_1|W}$ and $P_{X_2|W}$ follow the Bernoulli parameters \tilde{t}_w and \tilde{q}_w respectively. We will now refer to X_1, X_2 under U or under W to mean the obvious. Note that $P_{X_1|W=w}$ and $P_{X_1|W=-w}$ are identical up to substituting the probabilities of 0 and 1. Similarly, $P_{X_1+X_2|W=w}$ and $P_{X_1+X_2|W=-w}$ are identical up to substituting the probability assigned to 0 and 2. Hence, we clearly have that $H(X_1|W) = H(X_1|U)$ and $H(X_1 + X_2|W) = H(X_1 + X_2|U)$. For the same reason, $P_{X_1+X_2}(1)$ under U and $P_{X_1+X_2}(1)$ under W are the same. Furthermore, under W we have that $P_{X_1+X_2}(0) = P_{X_1+X_2}(2)$, and so by the grouping rule for entropy we conclude that $H(X_1 + X_2)$ under W is not smaller than $H(X_1 + X_2)$ under U . Moreover, from symmetry we have that $P_{X_1, X_2}(0, 1) = P_{X_1, X_2}(1, 0)$ under W . We can therefore think of X_1, X_2 under W as being generated by (11) for $\eta = \Pr(X_1 \neq X_2) = P_{X_1+X_2}(1)$. \square

We now restrict our attention to distributions of the form (11). Fix some η , and note that

$$H(X_1 + X_2) = h(\eta) + 1 - \eta = L(\eta). \quad (12)$$

Our goal is therefore to maximize $H(X_1 + X_2|U)$ subject to $H(X_1|U) \geq r_1$, over all $P_U, P_{X_1|U}, P_{X_2|U}$ for which P_{X_1, X_2} is consistent with (11) and our η .

Define

$$\begin{aligned} a_u &= \Pr(X_1 = 0|U = u) \\ b_u &= \Pr(X_2 = 0|U = u) \end{aligned}$$

and the random variables $a \triangleq a_U$ and $b \triangleq b_U$. Note that by definition

$$H(X_1|U) = \mathbb{E}h(a), \quad H(X_2|U) = \mathbb{E}h(b) \quad (13)$$

Clearly

$$H(X_1 + X_2|U = u) = H(a_u b_u, (1 - a_u)(1 - b_u), a_u \star b_u)$$

Moreover, by the grouping rule for entropy we can also write

$$\begin{aligned} H(X_1, X_2|U = u) &= H(a_u b_u, (1 - a_u)(1 - b_u), (1 - a_u)b_u, a_u(1 - b_u)) \\ &= H(a_u b_u, (1 - a_u)(1 - b_u), a_u \star b_u) + (a_u \star b_u)h\left(\frac{a_u(1 - b_u)}{a_u \star b_u}\right) \end{aligned}$$

Hence, noting that also $H(X_1, X_2|U = u) = h(a_u) + h(b_u)$ we obtain

$$H(X_1 + X_2|U = u) = F(a_u, b_u)$$

where

$$F(y, z) \triangleq h(y) + h(z) - (y \star z) \cdot h\left(\frac{y(1-z)}{y \star z}\right)$$

Our task is now reduced to upper bounding

$$\mathbb{E}F(a, b) = H(X_1 + X_2|U) \quad (14)$$

subject to the constraints

$$\begin{aligned} \mathbb{E}a &= \Pr(X_1 = 0) = \frac{1}{2} \\ \mathbb{E}b &= \Pr(X_2 = 0) = \frac{1}{2} \\ \mathbb{E}ab &= \Pr(X_1 = 0, X_2 = 0) = \frac{1}{2}(1 - \eta) \\ \mathbb{E}h(a) &\geq r_1 \end{aligned} \quad (15)$$

In [18], Wyner has upper bounded $\mathbb{E}h(a) + \mathbb{E}h(b)$ subject to the first three constraints. We extend his technique to account for the additional term and the additional entropy constraint.

The following proposition can be verified via standard analysis.

Proposition 4. *$F(y, z)$ is concave in the pair (y, z) . In addition $F(y, z) = F(z, y)$.*

Define the random variable $\gamma = \frac{a+b}{2}$, and note that $\mathbb{E}\gamma = \frac{1}{2}$. Using Proposition 4, we have that

$$\begin{aligned} \mathbb{E}F(a, b) &= \mathbb{E}\left(\frac{1}{2}F(a, b) + \frac{1}{2}F(b, a)\right) \\ &\leq \mathbb{E}F(\gamma, \gamma) \\ &= 2\mathbb{E}(h(\gamma) + \gamma^2 - \gamma) \\ &= -\frac{1}{2} + 2\mathbb{E}\left(h(\gamma) + (\gamma - \frac{1}{2})^2\right) \end{aligned} \quad (16)$$

Defining $\theta = |\gamma - \frac{1}{2}|$ and letting $G(y) = h(\sqrt{y} + \frac{1}{2}) + y$ we have that

$$\mathbb{E}F(a, b) \leq -\frac{1}{2} + 2\mathbb{E}G(\theta^2) \quad (17)$$

where we have used the symmetry of $h(\cdot)$ around $\frac{1}{2}$.

The following proposition can be verified via standard analysis.

Proposition 5. $G(y)$ is concave and monotone decreasing over $[0, \frac{1}{4}]$.

Using (17) and the concavity of $G(y)$ we obtain

$$\mathbb{E}F(a, b) \leq -\frac{1}{2} + 2\mathbb{E}G(\theta^2) \leq -\frac{1}{2} + 2G(\mathbb{E}\theta^2), \quad (18)$$

Since $G(y)$ is monotone decreasing, we can further upper bound (18) by replacing $\mathbb{E}\theta^2$ with any lower bound. To that end:

$$\mathbb{E}(\theta^2) = \mathbb{E}\left(\gamma - \frac{1}{2}\right)^2 = \mathbb{E}\gamma^2 - \mathbb{E}\gamma + \frac{1}{4} = \frac{1}{4}(\mathbb{E}(a+b)^2 - 1) \quad (19)$$

Hence, we need a lower bound on $\mathbb{E}(a+b)^2$, subject to the constraints (15).

Lemma 5. Let X, Y be two random variables satisfying $\mathbb{E}X^2 < \infty$ and $\mathbb{E}XY = \mu \geq 0$. Assume further that $X \in \mathcal{A}$ for some family \mathcal{A} . Define

$$\lambda^* \triangleq \max \left\{ \min_{X \in \mathcal{A}} \frac{\mu}{\mathbb{E}X^2}, 1 \right\}.$$

Then

$$\mathbb{E}(X+Y)^2 \geq \frac{(1+\lambda^*)^2}{\lambda^*} \mu$$

Proof. For any $X \in \mathcal{A}$ define $\lambda_X \triangleq \frac{\mu}{\mathbb{E}X^2}$. For any Y we can write

$$\begin{aligned} \mathbb{E}(X+Y)^2 &= \mathbb{E}(X + \lambda_X X + Y - \lambda_X X)^2 \\ &= (1 + \lambda_X)^2 \mathbb{E}X^2 + \mathbb{E}(Y - \lambda_X X)^2 + 2(1 + \lambda_X) \mathbb{E}X(Y - \lambda_X X) \\ &\geq (1 + \lambda_X)^2 \mathbb{E}X^2 \end{aligned}$$

where the last inequality follows since $\mathbb{E}XY = \lambda_X \mathbb{E}X^2 = \mu$. Therefore,

$$\mathbb{E}(X+Y)^2 \geq \frac{(1+\lambda_X)^2}{\lambda_X} \lambda_X \mathbb{E}X^2 = \frac{(1+\lambda_X)^2}{\lambda_X} \mu$$

Note that the function $K(\lambda) = \frac{(1+\lambda)^2}{\lambda}$ has a unique minimum at $\lambda = 1$. Define $\lambda^\dagger \triangleq \min_{X \in \mathcal{A}} \lambda_X$, and observe that $\lambda^* = \max\{\lambda^\dagger, 1\}$. Hence if $\lambda^\dagger > 1$ we can further lower bound the above by substituting $\lambda_X \rightarrow \lambda^\dagger$. Otherwise, we can replace λ_X by 1. \square

We would like to use Lemma 5 to lower bound $\mathbb{E}(a+b)^2$. To that end, define the zero mean random variables $\bar{a} = a - \frac{1}{2}$ and $\bar{b} = b - \frac{1}{2}$, and note that \bar{a} must satisfy $h(\bar{a} + \frac{1}{2}) \geq r_1$. In order to apply the lemma we first need to upper bound $\mathbb{E}\bar{a}^2$ under this latter restriction.

Lemma 6. *Let X be a zero mean random variable over $[-\frac{1}{2}, \frac{1}{2}]$ satisfying $\mathbb{E}h(X + \frac{1}{2}) \geq \rho$. Then $\mathbb{E}X^2 \leq (\frac{1}{2} - h^{-1}(\rho))^2$, and this bound is tight.*

Proof. Define $Q(y) = h(\frac{1}{2} - \sqrt{y})$. It is easily verified that $Q(y)$ is concave over $[0, \frac{1}{4}]$. Then

$$\rho \leq \mathbb{E}h\left(\frac{1}{2} - X\right) = \mathbb{E}Q(X^2) \leq Q(\mathbb{E}X^2) = h\left(\frac{1}{2} - \sqrt{\mathbb{E}X^2}\right).$$

Using the monotonicity of h^{-1} we get $\mathbb{E}X^2 \leq (\frac{1}{2} - h^{-1}(\rho))^2$. This bound is attained with equality by X uniformly distributed over $\{\frac{1}{2} - h^{-1}(\rho), h^{-1}(\rho) - \frac{1}{2}\}$. \square

Taking \mathcal{A} in Lemma 5 as the family of all random variables \bar{a} distributed over $[-\frac{1}{2}, \frac{1}{2}]$ with $h(\bar{a} + \frac{1}{2}) \geq r_1$, and noting that $\mathbb{E}\bar{a}\bar{b} = \frac{1}{4} - \frac{1}{2}\eta \geq 0$, we can use Lemma 6 to express the associated λ^* as

$$\begin{aligned} \lambda^* &= \max \left\{ \frac{\frac{1}{4} - \frac{1}{2}\eta}{\max_{\bar{a} \in \mathcal{A}} \mathbb{E}\bar{a}^2}, 1 \right\} = \max \left\{ \frac{\frac{1}{4} - \frac{1}{2}\eta}{(\frac{1}{2} - h^{-1}(r_1))^2}, 1 \right\} \\ &= \max \left\{ \frac{\frac{1}{2} - \eta}{\frac{1}{2} - h^{-1}(r_1) \star h^{-1}(r_1)}, 1 \right\} \end{aligned}$$

and hence if $h^{-1}(r_1) \star h^{-1}(r_1) > \eta$ then

$$\begin{aligned} \mathbb{E}(a + b)^2 &= 1 + \mathbb{E}(\bar{a} + \bar{b})^2 \geq 1 + \frac{(1 + \lambda^*)^2}{2\lambda^*} \left(\frac{1}{2} - \eta \right) \\ &= 1 + \frac{(1 - \eta - h^{-1}(r_1) \star h^{-1}(r_1))^2}{1 - 2(h^{-1}(r_1) \star h^{-1}(r_1))} \end{aligned}$$

and otherwise $\mathbb{E}(a + b)^2 \geq 1 + 4(\frac{1}{4} - \frac{1}{2}\eta)$. Combining this with (14), (18) and (19) we obtain

$$H(X_1 + X_2 | U) \leq -\frac{1}{2} + 2G\left(\frac{1}{4}(\mathbb{E}(a + b)^2 - 1)\right) \leq J(h^{-1}(r_1), \eta). \quad (20)$$

Remark 6. *The above bound can be attained whenever $\eta \geq h^{-1}(r_1) \star h^{-1}(r_1)$. To show this, we specify a distribution that satisfies (15) (and therefore also $H(X_1 + X_2) = h(\eta) + 1 - \eta$), and satisfies the bound (20) with equality. Let $p^* \leq \frac{1}{2}$ be such that $p^* \star p^* = \eta$, i.e., $p^* = \frac{1}{2}(1 - \sqrt{1 - 2\eta})$, and consider the following distribution:*

$$\begin{aligned} X_1 &= U \oplus Z_1, \quad X_2 = U \oplus Z_2 \\ U &\sim \text{Bern}\left(\frac{1}{2}\right), \quad Z_1 \sim \text{Bern}(p^*), \quad Z_2 \sim \text{Bern}(p^*) \end{aligned} \quad (21)$$

where U, Z_1, Z_2 are mutually independent. Note that $X_2 = X_1 \oplus Z$, where $Z = (Z_1 \oplus Z_2) \sim \text{Bern}(\eta)$. Hence, $\mathbb{E}X_1 = \mathbb{E}X_2 = \frac{1}{2}$ and $\Pr(X_1 = 0, X_2 = 0) = \frac{1}{2}(1 - \eta)$. Furthermore,

$$\begin{aligned} H(X_1 + X_2|U) &= \frac{1}{2}H(Z_1 + Z_2) + \frac{1}{2}H(2 - (Z_1 + Z_2)) = H(Z_1 + Z_2) \\ &= H(Z_1 + Z_2, Z_1) - H(Z_1|Z_1 + Z_2) = H(Z_1, Z_2) - H(Z_1|Z_1 + Z_2) \\ &= 2h(p^*) - \eta \cdot H(Z_1|Z_1 + Z_2 = 1) \\ &= 2h\left(\frac{1}{2}\left(1 - \sqrt{1 - 2\eta}\right)\right) - \eta \end{aligned}$$

Since $\eta = p^* \star p^* \geq h^{-1}(r_1) \star h^{-1}(r_1)$, we also have that $H(X_1|U) = h(p^*) \geq r_1$. Therefore this distribution indeed satisfies the constraints. For $\eta < h^{-1}(r_1) \star h^{-1}(r_1)$, it is believed that the bound (20) is not tight, due to the inequality in (16).

Finally, we show that the constraints (15) cannot be satisfied if $\eta < h^{-1}(r_1)$.

Lemma 7. *Let X and Y be two zero mean random variables on $[-\frac{1}{2}, \frac{1}{2}]$. If $\mathbb{E}h(Y + \frac{1}{2}) \geq \rho$ then $\mathbb{E}XY \leq \frac{1}{2}(\frac{1}{2} - h^{-1}(\rho))$.*

Proof. Clearly $\mathbb{E}X^2 \leq \frac{1}{4}$, and by Lemma 6 also $\mathbb{E}Y^2 \leq (\frac{1}{2} - h^{-1}(\rho))^2$. Using the Cauchy-Schwarz Inequality we have

$$(\mathbb{E}XY)^2 \leq \mathbb{E}X^2 \mathbb{E}Y^2 \leq \frac{1}{4} \left(\frac{1}{2} - h^{-1}(\rho) \right)^2$$

□

Using \bar{a}, \bar{b} in the above Lemma and recalling that $\mathbb{E}\bar{a}\bar{b} = \frac{1}{4} - \frac{1}{2}\eta$ and that $\mathbb{E}h(\bar{a} + \frac{1}{2}) \geq r_1$, we indeed verify that $\eta \geq h^{-1}(r_1)$ must hold.

The proof of Lemma 3 now follows since we have shown that for any admissible (r_0, r_1, r_2) , there must exist an $h^{-1}(r_1) \leq \eta \leq \frac{1}{2}$ such that $r_0 + r_1 + r_2 \leq L(\eta)$ and $r_1 + r_2 \leq J(p, \eta)$.

5 Discussion

Given a pair of multiset-union-free families $\mathcal{F}_1, \mathcal{F}_2$ of subsets of $[n]$ with cardinalities 2^{nR_1} and 2^{nR_2} respectively, we have introduced a bounding technique based on a procedure for constructing a multiset-union-free system \mathcal{U} over subsets of $[(1 - \alpha)n]$, for $\alpha < 1$. This was achieved by proving the existence of a subset $S \subset [n]$ of cardinality αn , such that the multiset-union of the projection multisets of each family on S , i.e., $P_S^+(\mathcal{F}_1) \uplus P_S^+(\mathcal{F}_2)$ has a member T with a large number of multiplicities, say $2^{n\rho}$. This in turn implied that $r_0 + r_1 + r_2$ for the system is at least $\rho/(1 - \alpha)$. To lower bound ρ as a function of α and the cardinalities of the original families, we introduced the soft Sauer-Perles-Shelah Lemma, which enabled us to bound the number of occurrences of the multiset $T = S$.

This lemma offered the additional benefit of a lower bound on r_1 . We note in passing that the bound obtained on R_2 as a function of R_1 outperforms previous results even without incorporating the constraint on r_1 . We suspect that better bounds on ρ can be obtained, possibly for T other than S .

References

- [1] Lindström, B. (1969) Determination of two vectors from the sum. *Journal of Combinatorial Theory* **6(4)** 402–407.
- [2] van Tilborg, H., (1978) An upper bound for codes in a two-access binary erasure channel (Corresp.). *IEEE Transactions on Information Theory* **24(1)** 112–116.
- [3] Kasami, T. and Lin, S. (1978) Bounds on the achievable rates of block coding for a memoryless multiple-access channel. *IEEE Transactions on Information Theory* **24(2)** 187–197.
- [4] Weldon, E.J. (1978) Coding for a multiple-access channel. *Information and Control* **36(3)** 256–274.
- [5] Kasami, T., Lin, S., Wei, V.K. and Yamamura, S. (1983) Graph theoretic approaches to the code construction for the two-user multiple-access binary adder channel *IEEE Transactions on Information Theory* **29(1)** 114–130.
- [6] van den Braak, P.C. and van Tilborg, H. (1985) A family of good uniquely decodable code pairs for the two-access binary adder channel. *IEEE Transactions on Information Theory* **31(1)** 3–9.
- [7] Bross, S. I. and Blake, I. F. (1998) Upper bound for uniquely decodable codes in a binary input N-user adder channel. *IEEE Transactions on Information Theory* **44(1)** 334–340.
- [8] Urbanke, R. and Li, Q. (1998) The zero-error capacity region of the 2-user synchronous BAC is strictly smaller than its Shannon capacity region. *Information Theory Workshop*, 61
- [9] Ahlswede, R. and Balakirsky, V.B. (1999) Construction of uniquely decodable codes for the two-user binary adder channel. *IEEE Transactions on Information Theory* **45(1)** 326–330.
- [10] Mattas, M. and Östergård, P.R.J. (2005) A New Bound for the Zero-Error Capacity Region of the Two-User Binary Adder Channel. *IEEE Transactions on Information Theory* **51(9)** 3289–3291.

- [11] Cover, T. M. and Thomas J. A. (1991) *Elements of Information Theory*. John Wiley and Sons.
- [12] Alon, N. and Spencer, J. H. (2004) *The probabilistic method*. John Wiley and Sons.
- [13] Alon, N. (1983) On the density of sets of vectors *Discrete Mathematics* **46(2)** 199–202.
- [14] Slepian, D. and Wolf J. K. (1973) A coding theorem for multiple access channels with correlated sources. *Bell System Technical Journal* **52(7)** 1037–1076.
- [15] Ahlswede, R. and Korner, J. (1975) Source coding with side information and a converse for degraded broadcast channels. *IEEE Transactions on Information Theory* **21(6)** 629–637.
- [16] Wyner, A. D. and Ziv, J. (1976). The rate-distortion function for source coding with side information at the decoder. *IEEE Transactions on Information Theory* **22(1)** 1–10.
- [17] Willems, F.M.J. (1982) Information theoretical results for the discrete memoryless multiple access channel. *Ph.D. dissertation*, Katholieke Universiteit Leuven, Belgium.
- [18] Wyner, A. D. (1975) The common information of two dependent random variables. *IEEE Transactions on Information Theory* **21(2)** 163–179.